UNCLASSIFIED

1 November 2015

NORTH DAKOTA

HOMELAND SECURITY

Cyber Summary

North Dakota State and Local Intelligence Center

NDSLIC

1-866-885-8295

The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC Disclaimer

The Cyber Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Table of Contents

North Dakota

Nothing Significant to Report

Regional

Nothing Significant to Report

National

(National) CIA director speaks out about email hack. The director of the CIA stated October 27 that the hack of his personal email account underlines that the fact that people are vulnerable to potentially having their personal information compromised on the Internet. The incident remains under investigation after the hacker allegedly reported the method of obtaining the sensitive information through an online publication. http://www.cbsnews.com/news/cia-director-john-brennan-speaks-out-on-email-hack/

International

(International) 12 new malware strands are discovered every minute. Security researchers at G DATA released report findings revealing that the company discovered 3,045,722 new types of malware in the first half of 2015, a 26.6 percent increase since the second half of 2014, and that most attacks were either adware or potentially unwanted programs (PUPs) hosted on U.S. Web sites from the healthcare and technology and telecommunications, among others. G DATA also observed an increase in banking trojan usage for the first time since 2012. http://news.softpedia.com/news/12-new-malware-strands-are-discovered-every-minute-495302.shtml

(International) Malware spread via black hat SEO campaign. Security researchers from Heimdal Security discovered a malware campaign in which criminals are using black hat search engine optimization (SEO) to distribute malicious software to technical users typing terms such as “Java JRE,” “MSN 7,” or “Windows 8,” into searches, which would then return infected Google top search results. http://news.softpedia.com/news/malware-spread-via-black-hat-seo-campaign-495195.shtml

(International) Russian trolls terrorize the West with old KGB methods. The activity of Russian trolls in the West has already gotten a lot of media coverage. However, sometimes it seems that the seriousness of the problem is underestimated both in Ukraine and in the European countries. http://euromaidanpress.com/2015/10/29/russian-trolls-terrorize-the-west-with-old-kgb-methods/

Banking and Finance Industry

Nothing Significant to Report

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

Nothing Significant to Report

Communications Sector

Nothing Significant to Report

Critical Manufacturing

(International) Internet-connected cars can be tracked by anyone, not just governments. A researcher from Security Innovation and the University of Twente discovered that smart cars using V2X technology could have their locations tracked using $550 Wi-Fi sniffers that have digital signatures unique to each vehicle. The National Highway Traffic Safety Administration and European authorities proposed that V2X transmitters utilize pseudonyms for vehicles to enhance security. http://news.softpedia.com/news/internet-connected-cars-can-be-tracked-by-anyone-not-just-governments-495161.shtml

(International) Hackers pop grease monkeys' laptops to disable Audi airbags. Security researchers from CrySyS Lab and Budapest University of Technology and Economics discovered that third party software used in certain Volkswagen Group vehicles could be compromised using a zero-day vulnerability, allowing an attacker to disable airbags and other car functions without mechanics' knowledge by falsifying car readouts via a malicious replaced dynamic link library (DLL) file used to communicate with the vehicle's diagnostic cable.
http://www.theregister.co.uk/\2015/10/23/hackers_pop_mechanics_laptops_to_silently_disable_car_airbags/

(International) Serious flaws found in Janitza power analyzers. Security researchers from Applied Risk discovered several vulnerabilities in Janitza power analyzer products, including an undocumented default password protecting a File Transfer Protocol (FTP) interface that could allow an attacker to upload and download arbitrary files, and a flaw in which an attacker could use a debug interface on Transmission Control Protocol (TCP) port 1239 to read and write files and execute JASIC code, among other issues. The vendor released firmware updates and new documentation addressing the issues; however researchers determined that not all flaws were effectively fixed.
http://www.securityweek.com/serious-flaws-found-janitza-power-analyzers

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

Nothing Significant to Report

Energy

Nothing Significant to Report

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

Nothing Significant to Report

Information Technology and Telecommunications

(International) CCTV cameras hijacked to form worldwide DDoS botnet. Security researchers from Incapsula discovered that hackers had used brute-force attacks to compromise over 900 closed circuit television (CCTV) cameras running the BusyBox operating system (OS) and install malware derived from ELF_BASHLITE to launch distributed denial-of-service (DDoS) attacks using Hypertext Transfer Protocol (HTTP) GET request floods. One device was recorded sending over 20,000 HTTP requests per second. http://news.softpedia.com/news/cctv-cameras-hijacked-to-form-worldwide-ddos-botnet-495166.shtml

(International) Joomla update patches critical SQL injection vulnerability. Joomla developers released an update to its content management system (CMS) addressing a Structured Query Language (SQL) injection vulnerability which could

allow an attacker to gain access to data in a Web site's backend, due to code in a Hypertext Preprocessor (PHP) file in Joomla's Administrator folder. The update also addressed two sets of inadequate access control list (ACL) checks that could have allowed potential read access to restricted data.
https://threatpost.com/joomla-update-patches-critical-sql-injection-vulnerability/115142/

(International) **Joomla flaw exploited in the wild within hours of disclosure.** Security researchers from Sucuri reported that malicious actors started exploiting critical vulnerabilities, including a Structured Query Language (SQL) injection issue in Joomla, within 4 hours of patches released by developers addressing the issue and subsequent flaw disclosures by researchers at Trustwave. The SQL injection vulnerability could allow a remote attacker to hijack administrator sessions and gain access to affected Joomla Web sites.
http://www.securityweek.com/joomla-flaw-exploited-wild-within-hours-disclosure

(International) **Adobe patches critical vulnerability in Shockwave Player.** Adobe released a patch resolving a memory corruption vulnerability in its Shockwave Player 12.2.0.162 for Windows and Mac user after researchers from Fortinet's Fortiguard Labs discovered that the vulnerability allowed attackers to compromise remote computers and execute remote code, allowing full control of the operating system without the victim being aware.
http://www.securityweek.com/adobe-patches-critical-vulnerability-shockwave-player

(International) **Flaws in Rockwell PLCs expose operational networks.** Rockwell Automation released firmware updates and mitigations addressing several vulnerabilities in its 1400 programmable logic controllers (PLCs) and its MicroLogix 1100 products including a buffer overflow bug that remotely crashes affected devices or executes arbitrary code, and a denial-of-service (DoS) bug dubbed "FrostyURL" that can be exploited to crash MicroLogix PLCs via a specially crafted uniform resource locator (URL) sent to victims through email, and a cross-site scripting (XSS) vulnerability that can be exploited to inject malicious JavaScript code in a device's Web server, among others.
http://www.securityweek.com/flaws-rockwell-plcs-expose-operational-networks

(International) 13 million passwords leaked from free hosting service. A security expert reported October 28 that 13 million personal user records including names, emails, and plaintext passwords from the free web hosting service, 000webhost.com were compromised after its main server was exploited via a flaw in its old version of PHP. To mitigate future breaches, 000webhost updated its systems, increased its encryption, and changed all passwords. http://www.securityweek.com/13-million-passwords-leaked-free-hosting-service

(International) Infinite Automation patches flaws in SCADA/HMI product. Infinite Automation Systems released an updated version of its Mango Automation product patching a series of vulnerabilities after researchers from ICS-CERT discovered unrestricted fire upload, information exposure, SQL injection, and cross-site scripting vulnerabilities. The version fixed all the flaws except an OS command injection and a cross-site request forgery (CSRF) flaw. http://www.securityweek.com/infinite-automation-patches-flaws-scadahmi-product

(International) New types of reflection DDoS attacks spotted. Akamai's Security Intelligence Response Team released a new threat advisory detailing 3 new types of reflection distributed denial-of-service (DDoS) attacks abusing the remote procedure call (RPC) portmap service with attacks exceeding 100 Gbps; Network Basic Input/Output System (NetBIOS) name servers with the largest attack peaking at 15.7 Gbps; and Sentinel license servers with peak bandwidth attacks of 11.7 Gbps.
http://www.securityweek.com/new-types-reflection-ddos-attacks-spotted

US-Cert Updates and Vulnerabilities

ACSC Releases 2015 Threat Report. The Australian Cyber Security Centre (ACSC) has released its 2015 Threat Report. This report provides threat information that Australian organizations are facing, such as cyber espionage, cyber attacks, and cyber crime. Mitigation and remediation steps are also included to assist organizations with preventing and responding to such threats. https://www.us-cert.gov/ncas/current-activity/2015/11/02/ACSC-Releases-2015-Threat-Report

ICS-CERT ALERTS & ADVISORIES

The Water ISAC has published a joint product with ICS-CERT, IT-ISAC, Multi-State ISAC, and FBI input.
Find it posted on the ICS-CERT web site at: https://ics-cert.us-cert.gov/Other-Reports

PUBLIC HEALTH

Nothing Significant to Report

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165